

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE
BOARD OF PATENT APPEALS AND INTERFERENCES**

APPLICANT(S): Jung-Soo JUNG, et al.

GROUP ART UNIT: 2136

APPLICATION NO.: 10/822,068

EXAMINER: LOUIE, OSCAR A.

FILING DATE: April 9, 2004

DOCKET: 678-1443 (P11789)

DATE: May 6, 2008

**FOR: METHOD AND SYSTEM FOR PROVIDING BROADCAST SERVICE
USING ENCRYPTION IN A MOBILE COMMUNICATION TERMINAL**

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' BRIEF ON APPEAL

REAL PARTY IN INTEREST

The real party in interest is Samsung Electronics Co, Ltd, the assignee of the subject application, having an office at 416, Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do, Republic of Korea.

RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge and belief, there are no currently pending related appeals, interferences or judicial proceedings.

STATUS OF CLAIMS

Original Claims 1-36 were filed in this application on April 9, 2004. Claims 8 and 15 were cancelled and Claims 1, 3, 4, 9, 11, 12, 17, 19, 20, 22, 24, 25, 29, 30 and 31 were amended in an Amendment filed August 30, 2007. Claims 1, 9, and 17 were amended in an after-Final Amendment filed January 31, 2008. Thus, Claims 1-7, 9-14 and 16-36 are pending in the Appeal. Claims 1, 9, 17, 19, 20, 22, 24, 25 and 31 are in independent form. For the purposes of this Appeal, Claims 1-7 stand or fall together, Claims 9-14 and 16 stand or fall together, Claims 17-18 stand or fall together, Claims 20-21 stand or fall together, Claims 22-23 stand or fall together, Claims 25-30 stand or fall together and Claims 31-36 stand or fall together.

STATUS OF AMENDMENTS

Thus, the Appendix to this Appeal Brief includes Claims 1-7, 9-14 and 16-36, with the status of Claims 1, 3, 4, 11, 12, 19, 20, 22, 24, 25, 29, 30 and 31 being indicated as “Previously Presented”, the status of Claims 9 and 17 being indicated as “Currently Amended”, and the status of Claims 2, 5-7, 10, 13, 14, 16, 18, 21, 23, 26-28 and 32-36 being indicated as “Original”.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention as recited in Claim 1 relates to a method for receiving the broadcast service in a mobile station, in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station (Specification at page 9, lines 1-27; page 11, line 26 to page 12, line 8; page 15, lines 11-19; FIG. 1)¹. The method includes generating a registration message including a predetermined registration identifier for identification of the encryption information, and transmitting the generated registration message to

¹ Although a citation for each feature of the claims is provided herein, Appellants do not concede the fact that support may be found elsewhere in the written description.

a base station (Specification at page 21, lines 25 to page 22, line 4, FIG. 12). The method also includes receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station (Specification at page 22, lines 4-10; page 30, lines 13-27; FIG. 13). The method further includes updating the registration identifier based on the updated encryption information (Specification at page 29, line 22 to page 30, line 1; FIG. 3).

The invention as recited in Claim 9 relates to a method for providing by a base station the broadcast service to a mobile station in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel (Specification at page 9, lines 1-27; FIG. 1). The method includes receiving a registration message transmitted from the mobile station (Specification at page 21, line 25 to page 22, line 4, FIG. 12). The method also includes determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different from a currently valid registration identifier (Specification at page 22, lines 4-10; FIG. 13). The method further includes transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station (Specification at page 30, lines 13-27, FIG. 13).

The invention as recited in Claim 17 relates to a method for receiving the broadcast service in a mobile station, in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station (Specification at page 9, lines 1-27; page 11, line 26 to page 12, line 8; page 15, lines 11-19; FIG. 1). The method includes generating a registration message including a predetermined mask key request bit for requesting transmission of predetermined mask key for decryption of the broadcast data and transmitting the generated registration message to a base station while the mobile station is using a broadcast service (Specification at page 21, lines 25 to page 22, line 4, FIG. 12). The method also includes receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit

(Specification at page 22, lines 4-10; page 30, lines 13-27; page 28, line 23 to page 29, line 6; FIG. 13).

The invention as recited in Claim 19 relates to a method for providing a broadcast service to at least one mobile station over a radio channel, a method for providing by a base station the broadcast service to a mobile station in a wireless communication system (Specification at page 9, lines 1-27; FIG. 1). The method includes receiving a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data, from the mobile station (Specification at page 21, lines 25 to page 22, line 4, FIG. 12). The method also includes analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key (Specification at page 30, lines 2-21; FIG. 13). The method further includes transmitting the encryption information to the mobile station when the base station determines to transmit the encryption information (Specification at page 30, lines 22-27; FIG. 13).

The invention as recited in Claim 20 relates to a method for receiving the broadcast service in the mobile station, in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data sequentially is encrypted with different encryption information and provided to a mobile station (Specification at page 9, lines 1-27; page 11, line 26 to page 12, line 8; page 15, lines 11-19; FIG. 1). The method includes generating a registration message for use of the broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires (Specification at page 31, line 20 to page 32, line 1, FIG. 14). The method further includes receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message (Specification at page 32, lines 7-18, FIG. 14). The method further includes continuously decrypting the broadcast data using the next encryption information when the lifetime of the current encryption information expires (Specification at page 33, line 21 to page 34, line 3, FIG. 14).

The invention as recited in Claim 22 relates to a method for The invention as recited in Claim 22 relates to a method for providing by a base station the broadcast service to a mobile station in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel (Specification at page 9, lines 1-27; FIG. 1). The method includes receiving a registration message for use of the broadcast service by the mobile station (Specification at page 21, line 25 to page 22, line 4, FIG. 12). The method further includes transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires (Specification at page 32, lines 7-18, FIG. 14).

The invention as recited in Claim 24 relates to a method for providing by a base station the broadcast service to a mobile station in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel (Specification at page 9, lines 1-27; FIG. 1). The method includes receiving a predetermined registration message for use of the broadcast service by the mobile station (Specification at page 21, line 25 to page 22, line 4, FIG. 12). The method further includes transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires (Specification at page 32, lines 7-18, FIG. 14).

The invention as recited in Claim 25 relates to a broadcast service in a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station (Specification at page 9, lines 1-27; page 11, line 26 to page 12, line 8; page 15, lines 11-19; FIG. 1). The method includes transmitting, by the mobile station, a first registration message for initial use of the broadcast service to the base station (Specification at page 21, line 25 to page 22, line 4, FIG. 12). The

method also includes upon receiving the first registration message, transmitting by the base station encryption information for decryption of the broadcast data to the mobile station (Specification at page 30, lines 2-12, FIG. 13). The method further includes upon receiving the encryption information, generating by the mobile station a registration identifier, which includes identification information of the encryption information (Specification at page 29, lines 20-21). The method further includes generating by the mobile station a second registration message including the registration identifier and transmitting the generated second registration message to the base station if second or later registration for use of the broadcast service by the mobile station is required (Specification at page 29, lines 13-19, FIG. 12). The method further includes comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station (Specification at page 30, lines 13-21; FIG. 13). The method further includes transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station (Specification at page 30, line 22 to page 31, line 7, FIG. 13).

The invention as recited in Claim 31 relates to a system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station (Specification at page 9, lines 1-27; page 11, line 26 to page 12, line 8; page 15, lines 11-19; FIG. 1). The system includes at least one mobile station connected to the base station through the radio channel, for performing location registration for use of the broadcast service, decrypting the broadcast data using the encryption information transmitted via the base station while using the broadcast service, generating a registration identifier as identification information of the encryption information, and transmitting the generated registration identifier to the base station (Specification at page 29, line 11 to page 30, line 1, FIG. 12). The system further includes at least one base station for transmitting to the mobile station broadcast data transmitted via the packet data service node while the mobile station is using the broadcast service, receiving a predetermined registration message transmitted during location registration of the mobile station,

analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station (Specification at page 30, line 2 to page 31, line 7, FIG. 13).

GROUND FOR REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 1-7, 9-14 and 16-36 under 35 U.S.C. §103(a) are rendered obvious over U.S. Patent No. 6,707,915 (Jobst).

ARGUMENT

1. Independent Claim 1 is patentable over Jobst

Independent Claim 1 was rejected as being obvious over Jobst.²

The invention as recited in Claim 1 relates to a method for receiving the broadcast service in a mobile station, in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station. The method includes generating a registration message including a predetermined registration identifier for identification of the encryption information, and transmitting the generated registration message to a base station. The method also includes receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station. The method further includes updating the registration identifier based on the updated encryption information.

Jobst discloses a method of transferring a data packet from a providing communication terminal.

1 A. Jobst does not teach or disclose receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station and updating the registration identifier based on the updated encryption information, and therefore Jobst cannot render Claim 1 unpatentable

² See Office Action dated November 1, 2007, at pages 3-5.

Claim 1 recites, in part, receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station and updating the registration identifier based on the updated encryption information. The Examiner relies on Jobst for rejecting these features.³

Jobst discloses a method of transferring a data packet from a providing communication terminal to a requesting communication terminal for securing a terminal against unauthorized software loading onto the phone. More particularly, a first signature is calculated using a Phone Password and a binary code of the file to be transmitted in the middle, and then the calculated first signature with the binary code of the file is transferred to a requesting phone. The requesting phone calculates a second signature based on the received binary code and previously stored Phone Password. After comparing the calculated second signature with the received first signature, the phone deems a response message to be coming from an authorized provider, if the two signatures are identical. In other words, such a comparison between the two signatures is for confirming whether it is an authorized provider for a certain selected software download because the two signatures are generated using a same signature generating algorithm. Further, the two signatures themselves are limited to be factors compared and are unique for the specific software transfer based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code. If the two signatures are not identical, the downloaded software would automatically have been deleted, not updated.⁴

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station. Jobst does not teach or disclose updating the registration identifier based on the updated encryption information.

The Examiner agreed that Jobst does not explicitly disclose receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid

³ See Office Action dated November 1, 2007, at page 5.

in the base station and updating the registration identifier based on the updated encryption information. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station and updating the registration identifier based on the updated encryption information" in the invention as disclosed by Jobst since multiple digital signatures may be used in the process of validation and decryption of information where a second digital signature may be based on some aspect of the first digital signature. The Examiner also states that Jobst does suggest two digital signatures that each possesses unique information.⁵ A rejection based on "may" and "two digital signatures that each possesses unique information" to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station and updating the registration identifier based on the updated encryption information, as recited by Claim 1.

Since Jobst does not teach or suggest the recitation of Claim 1 of the present application, i.e., receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station and updating the registration identifier based on the updated encryption information, Claim 1 cannot be rendered obvious over Jobst.

Based on at least the foregoing it is respectfully submitted that the rejection of Claim 1 under 35 U.S.C. §103(a) must be reversed.

1B. Independent Claim 1 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 1, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner

⁴ See Jobst, at column 6, line 57 to column 8, line 27.

has failed to make out a prima facie case for an obviousness rejection, and thus Claim 1 is allowable.

1C. Dependent Claims 2-7 are patentable over Jobst

Without conceding the patentability per se of dependent Claims 2-7, these claims are likewise believed to be allowable by virtue of at least their dependence on Claim 1.

2. Independent Claim 9 is patentable over Jobst

Independent Claim 9 was rejected as being obvious over Jobst.⁶

The invention as recited in Claim 9 relates to a method for providing by a base station the broadcast service to a mobile station in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel. The method also includes determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different from a currently valid registration identifier. The method further includes transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station.

Jobst discloses a method of transferring a data packet from a providing communication terminal.

2A. Jobst does not teach or disclose determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different from a currently valid registration identifier and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station, and therefore Jobst cannot render Claim 9 unpatentable

Claim 9 recites, in part, determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different

⁵ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

from a currently valid registration identifier and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station. The Examiner relies on Jobst for rejecting these features.⁷

Jobst discloses a method of transferring a data packet from a providing communication terminal to a requesting communication terminal for securing a terminal against unauthorized software loading onto the phone. More particularly, a first signature is calculated using a Phone Password and a binary code of the file to be transmitted in the middle, and then the calculated first signature with the binary code of the file is transferred to a requesting phone. The requesting phone calculates a second signature based on the received binary code and previously stored Phone Password. After comparing the calculated second signature with the received first signature, the phone deems a response message to be coming from an authorized provider, if the two signatures are identical. In other words, such a comparison between the two signatures is for confirming whether it is an authorized provider for a certain selected software download because the two signatures are generated using a same signature generating algorithm. Further, the two signatures themselves are limited to be factors compared and are unique for the specific software transfer based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code. If the two signatures are not identical, the downloaded software would automatically have been deleted, not updated.⁸

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different from a currently valid registration identifier. Jobst does not teach or disclose transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station.

The Examiner agreed that Jobst does not explicitly disclose determining whether a registration identifier for identification of encryption information required for decryption of the

⁶ See Office Action dated November 1, 2007, at pages 3 and 9-11.

⁷ See Office Action dated November 1, 2007, at pages 10-11.

⁸ See Jobst, at column 6, line 57 to column 8, line 27.

broadcast data is included in the registration message, determining whether it is necessary to transmit updated encryption information to the mobile station and transmitting updated encryption information to the mobile station according to the determination result when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "determining whether a registration identifier for identification of encryption information required for decryption of the broadcast data is included in the registration message, determining whether it is necessary to transmit updated encryption information to the mobile station and transmitting updated encryption information to the mobile station according to the determination result when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station" as disclosed by Jobst since the base station would have to receive a transmission from a mobile device in order to authenticate and determine whether it is valid. The Examiner also states that Jobst does suggest two digital signatures that each possesses unique information.⁹ A rejection based on "would have to" and "two digital signatures that each possesses unique information" to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different from a currently valid registration identifier and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station, as recited by Claim 9.

Since Jobst does not teach or suggest the recitation of Claim 9 of the present application, i.e., determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different from a currently valid registration identifier and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration

⁹ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

identifier currently valid in the base station, Claim 9 cannot be rendered obvious over Jobst.

Based on at least the foregoing it is respectfully submitted that the rejection of Claim 9 under 35 U.S.C. §103(a) must be reversed.

2B. Independent Claim 9 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 9, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 9 is allowable.

2C. Dependent Claims 10-14 and 16 are patentable over Jobst

Without conceding the patentability per se of dependent Claims 10-14 and 16, these claims are likewise believed to be allowable by virtue of at least their dependence on Claim 9.

3. Independent Claim 25 are patentable over Jobst

Independent Claim 25 was rejected as being obvious over Jobst.¹⁰

The invention as recited in Claim 25 relates to a broadcast service in a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station. The method includes transmitting, by the mobile station, a first registration message for initial use of the broadcast service to the base station. The method also includes upon receiving the first registration message, transmitting by the base station encryption information for decryption of the broadcast data to the mobile station. The method further includes upon receiving the encryption information, generating by the mobile station a registration identifier, which includes identification information of the encryption information. The method further includes generating by the mobile station a second registration message including the registration identifier and transmitting the generated second

¹⁰ See Office Action dated November 1, 2007, at pages 3 and 23-26.

registration message to the base station if second or later registration for use of the broadcast service by the mobile station is required. The method further includes comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station. The method further includes transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station.

Jobst discloses a method of transferring a data packet from a providing communication terminal.

3A. Jobst does not teach or disclose comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station, and therefore Jobst cannot render Claim 25 unpatentable

Claim 25 recites, in part, comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station. The Examiner relies on Jobst for rejecting these features.¹¹

Jobst discloses a method of transferring a data packet from a providing communication terminal to a requesting communication terminal for securing a terminal against unauthorized software loading onto the phone. More particularly, a first signature is calculated using a Phone Password and a binary code of the file to be transmitted in the middle, and then the calculated first signature with the binary code of the file is transferred to a requesting phone. The requesting phone calculates a second signature based on the received binary code and previously stored Phone

¹¹ See Office Action dated November 1, 2007, at pages 25-26.

Password. After comparing the calculated second signature with the received first signature, the phone deems a response message to be coming from an authorized provider, if the two signatures are identical. In other words, such a comparison between the two signatures is for confirming whether it is an authorized provider for a certain selected software download because the two signatures are generated using a same signature generating algorithm. Further, the two signatures themselves are limited to be factors compared and are unique for the specific software transfer based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code. If the two signatures are not identical, the downloaded software would automatically have been deleted, not updated.¹²

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station.

The Examiner agreed that Jobst does not explicitly disclose comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station" as disclosed by Jobst since a phone may send various forms of authentication information (i.e., encryption/decryption information, unique identifiers, keys, certificates, signatures, etc). The

¹² See Jobst, at column 6, line 57 to column 8, line 27.

Examiner also states that Jobst does suggest two digital signatures that each possesses unique information.¹³ A rejection based on “may” and “two digital signatures that each possesses unique information” to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station, as recited by Claim 25.

Since Jobst does not teach or suggest the recitation of Claim 25 of the present application, of comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station and transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station, Claim 25 cannot be rendered obvious over Jobst.

Based on at least the foregoing it is respectfully submitted that the rejection of Claim 25 under 35 U.S.C. §103(a) must be reversed.

3B. Independent Claim 25 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 25, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 25 is allowable.

3C. Dependent Claims 26-30 are patentable over Jobst

Without conceding the patentability per se of dependent Claims 26-30, these claims are likewise believed to be allowable by virtue of at least their dependence on Claim 25.

¹³ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

4. Independent Claim 31 are patentable over Jobst

Independent Claim 31 was rejected as being obvious over Jobst.¹⁴

The invention as recited in Claim 31 relates to a system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station. The system includes at least one mobile station connected to the base station through the radio channel, for performing location registration for use of the broadcast service, decrypting the broadcast data using the encryption information transmitted via the base station while using the broadcast service, generating a registration identifier as identification information of the encryption information, and transmitting the generated registration identifier to the base station. The system further includes at least one base station for transmitting to the mobile station broadcast data transmitted via the packet data service node while the mobile station is using the broadcast service, receiving a predetermined registration message transmitted during location registration of the mobile station, analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station.

Jobst discloses a method of transferring a data packet from a providing communication terminal.

4A. Jobst does not teach or disclose analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station, and therefore Jobst cannot render Claim 31 unpatentable

Claim 31 recites, in part, analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the

encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station. The Examiner relies on Jobst for rejecting these features.¹⁵

Jobst discloses a method of transferring a data packet from a providing communication terminal to a requesting communication terminal for securing a terminal against unauthorized software loading onto the phone. More particularly, a first signature is calculated using a Phone Password and a binary code of the file to be transmitted in the middle, and then the calculated first signature with the binary code of the file is transferred to a requesting phone. The requesting phone calculates a second signature based on the received binary code and previously stored Phone Password. After comparing the calculated second signature with the received first signature, the phone deems a response message to be coming from an authorized provider, if the two signatures are identical. In other words, such a comparison between the two signatures is for confirming whether it is an authorized provider for a certain selected software download because the two signatures are generated using a same signature generating algorithm. Further, the two signatures themselves are limited to be factors compared and are unique for the specific software transfer based on a sequence specific for the receiving phone and a sequence specific for the transmitted software code. If the two signatures are not identical, the downloaded software would automatically have been deleted, not updated.¹⁶

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose analyzing a registration identifier of the encryption information included in the predetermined registration message. Jobst does not teach or disclose determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station.

The Examiner agreed that Jobst does not explicitly disclose analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the encryption information for the mobile station when the

¹⁴ See Office Action dated November 1, 2007, at pages 3 and 31-32.

¹⁵ See Office Action dated November 1, 2007, at page 32.

¹⁶ See Jobst, at column 6, line 57 to column 8, line 27.

registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station" as disclosed by Jobst since it is necessary to have at least one mobile station and at least one base station in a communications network in order to have any type of operable system with procedures for authentication and encryption. The Examiner also states that Jobst does suggest two digital signatures that each possesses unique information.¹⁷ A rejection based on "two digital signatures that each possesses unique information" to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station, as recited by Claim 31.

Since Jobst does not teach or suggest the recitation of Claim 31 of the present application, of analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station, Claim 31 cannot be rendered obvious over Jobst.

Based on at least the foregoing it is respectfully submitted that the rejection of Claim 31 under 35 U.S.C. §103(a) must be reversed.

¹⁷ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

4B. Independent Claim 31 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 31, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 31 is allowable.

4C. Dependent Claims 32-36 are patentable over Jobst

Without conceding the patentability per se of dependent Claims 32-36, these claims are likewise believed to be allowable by virtue of at least their dependence on Claims 31.

5. Independent Claims 17 is patentable over Jobst

Independent Claims 17 was rejected as being obvious over Jobst.¹⁸

The invention as recited in Claim 17 relates to a method for receiving the broadcast service in a mobile station, in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station. The method includes generating a registration message including a predetermined mask key request bit for requesting transmission of predetermined mask key for decryption of the broadcast data and transmitting the generated registration message to a base station while the mobile station is using a broadcast service. The method also includes receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit.

Jobst discloses a method of transferring a data packet from a providing communication terminal.

5A. Jobst does not teach or disclose encryption information including a predetermined mask key and lifetime information of the predetermined mask key in a wireless communication system.

¹⁸ See Office Action dated November 1, 2007, at pages 3 and 15-16.

wherein broadcast data is sequentially encrypted with different encryption information, and therefore Jobst cannot render Claim 17 unpatentable

Claim 17 recites, in part, receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit. The Examiner relies on Jobst for rejecting these features.¹⁹

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit.

The Examiner agreed that Jobst does not explicitly disclose receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit" as disclosed by Jobst since multiple digital signatures may be used in the process of validation and decryption of information where a second digital signature may be based on some aspect of the first digital signature. The Examiner also states that Jobst does suggest encryption information and unique identification codes.²⁰ A rejection based on "may be" and "encryption information and unique identification codes" to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit, as recited by Claim 17.

Since Jobst does not teach or suggest the recitation of Claim 17 of the present application, of receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit.

¹⁹ See Office Action dated November 1, 2007, at pages 15-16.

Based on at least the foregoing it is respectfully submitted that the rejection of Claim 17 under 35 U.S.C. §103(a) must be reversed.

5B. Independent Claim 17 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 17, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 17 is allowable.

5C. Dependent Claim 18 is patentable over Jobst

Without conceding the patentability per se of dependent Claim 18, this claim is likewise believed to be allowable by virtue of at least its dependence on Claim 17.

6. Independent Claim 19 is patentable over Jobst

Independent Claim 19 was rejected as being obvious over Jobst.²¹

The invention as recited in Claim 19 relates to a method for providing a broadcast service to at least one mobile station over a radio channel, a method for providing by a base station the broadcast service to a mobile station in a wireless communication system. The method includes receiving a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data, from the mobile station. The method also includes analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key. The method further includes transmitting the encryption information to the mobile station when the base station determines to transmit the encryption information.

Jobst discloses a method of transferring a data packet from a providing communication terminal.

²⁰ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

²¹ See Office Action dated November 1, 2007, at pages 3 and 17-18.

6A. Jobst does not teach or disclose encryption information including the predetermined mask key and lifetime information of the predetermined mask key in a wireless communication system, wherein broadcast data is sequentially encrypted with different encryption information, and therefore Jobst cannot render Claim 19 unpatentable

Claim 19 recites, in part, analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key. The Examiner relies on Jobst for rejecting these features.²²

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key. The Examiner relies on Jobst for rejecting these features.

The Examiner agreed that Jobst does not explicitly disclose analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key" as disclosed by Jobst since the analysis of various conditions of data (i.e., values, keys, certificates, signatures, etc.) is typical for multi-tiered/layered authentication procedures. The Examiner also states that Jobst does suggest encryption information and unique identification codes.²³ A rejection based on "encryption information and unique identification codes" to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key, as recited by

²² See Office Action dated November 1, 2007, at page 18.

Claim 19.

Since Jobst does not teach or suggest the recitation of Claim 19 of the present application, of analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key.

Based on at least the foregoing it is respectfully submitted that the rejection of Claim 19 under 35 U.S.C. §103(a) must be reversed.

6C. Independent Claim 19 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 19, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 19 is allowable.

7. Independent Claim 20 is patentable over Jobst

Independent Claim 20 was rejected as being obvious over Jobst.²⁴

The invention as recited in Claim 20 relates to a method for receiving the broadcast service in the mobile station, in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data sequentially is encrypted with different encryption information and provided to a mobile station. The method includes generating a registration message for use of the broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires. The method further includes receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message. The method further includes continuously decrypting the broadcast data using the next encryption information when the lifetime of the current encryption information expires.

Jobst discloses a method of transferring a data packet from a providing communication

²³ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

²⁴ See Office Action dated November 1, 2007, at pages 3 and 18-20.

terminal.

7A. Jobst does not teach or disclose encryption information including a predetermined mask key and lifetime information of the corresponding predetermined mask key in a wireless communication system, wherein broadcast data is sequentially encrypted with different encryption information, and therefore Jobst cannot render Claim 20 unpatentable

Claim 20 recites, in part, generating a registration message for use of the broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires. The Examiner relies on Jobst for rejecting these features.²⁵

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose generating a registration message for use of the broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires.

The Examiner agreed that Jobst does not explicitly disclose generating a registration message for use of the broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "generating a registration message for use of the broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires" as disclosed by Jobst since prior to the transmission of a message it must be generated and may be generated with different types of data (i.e. unique identification information, etc). The Examiner also states that Jobst does suggest encryption information and unique identification codes.²⁶ A rejection based on "may be" and "encryption information and unique identification codes" to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest generating a registration message for use of

²⁵ See Office Action dated November 1, 2007, at pages 19-20.

the broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires, as recited by Claim 20.

7B. Jobst does not teach or disclose receiving both current encryption information and next encryption information, and therefore receiving/transmitting both current encryption information and next encryption information cannot render Claim 20 unpatentable

Claim 20 recites, in part, receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message. The Examiner relies on Jobst for rejecting these features.²⁷

Jobst discloses a method of transferring a data packet from a providing communication terminal to a requesting communication terminal for securing a terminal against unauthorized software loading onto the phone. More particularly, Jobst uses a unique identification code to verify the identity of the requesting communication terminal and thereby check whether the data packet is provided by an authorized provider or not.

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message.

The Examiner agreed that Jobst does not explicitly disclose receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message" as disclosed by Jobst since it is obvious for a terminal (i.e. mobile station) to continuously use the existing encryption/decryption information to decrypt data unless otherwise informed of an encryption key change. The Examiner also states that Jobst does suggest a first digital signature and a second digital signature. A rejection based on "a first digital signature and a second digital signature" to

²⁶ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message, as recited by Claim 20.

Since Jobst does not teach or suggest the recitation of Claim 20 of the present application, of receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message.

Based on at least the foregoing it is respectfully submitted that the rejection of Claim 20 under 35 U.S.C. §103(a) must be reversed.

7C. Independent Claim 20 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 20, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 20 is allowable.

7D. Dependent Claim 21 is patentable over Jobst

Without conceding the patentability per se of dependent Claim 21, this claim is likewise believed to be allowable by virtue of at least its dependence on Claim 20.

8. Independent Claim 22 is patentable over Jobst

Independent Claim 22 was rejected as being obvious over Jobst.²⁸

The invention as recited in Claim 22 relates to a method for The invention as recited in Claim 22 relates to a method for providing by a base station the broadcast service to a mobile station in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel. The method includes receiving a registration message for use of the broadcast service by the mobile station. The method further includes transmitting current

²⁷ See Office Action dated November 1, 2007, at page 20.

²⁸ See Office Action dated November 1, 2007, at pages 3 and 21-22.

encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires.

Jobst discloses a method of transferring a data packet from a providing communication terminal.

8A. Jobst does not teach or disclose transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires cannot render Claim 22 unpatentable

Claim 22 recites, in part, transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires. The Examiner relies on Jobst for rejecting these features.²⁹

Jobst discloses a method of transferring a data packet from a providing communication terminal to a requesting communication terminal for securing a terminal against unauthorized software loading onto the phone. More particularly, Jobst uses a unique identification code to verify the identity of the requesting communication terminal and thereby check whether the data packet is provided by an authorized provider or not.

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires.

The Examiner agreed that Jobst does not explicitly disclose transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires. However, the Examiner states that it would

²⁹ See Office Action dated November 1, 2007, at pages 21-21.

have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires" as disclosed by Jobst since a base station transmitting a message to a communication terminal (i.e., mobile station) would have to be received in order to authenticate and verify the communication terminal, prior to the transmission of encryption/decryption information. The Examiner also states that Jobst does suggest a first digital signature and a second digital signature.³⁰ A rejection based on "a first digital signature and a second digital signature" to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires, as recited by Claim 22.

Since Jobst does not teach or suggest the recitation of Claim 22 of the present application, of transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires. Based on at least the foregoing it is respectfully submitted that the rejection of Claim 22 under 35 U.S.C. §103(a) must be reversed.

8B. Independent Claim 22 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 22, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 22 is allowable.

³⁰ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

8C. Dependent Claim 23 is patentable over Jobst

Without conceding the patentability per se of dependent Claim 23, this claim is likewise believed to be allowable by virtue of at least its dependence on Claim 23.

9. Independent Claim 24 is patentable over Jobst

Independent Claim 24 was rejected as being obvious over Jobst.³¹

The invention as recited in Claim 24 relates to a method for providing by a base station the broadcast service to a mobile station in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel. The method includes receiving a predetermined registration message for use of the broadcast service by the mobile station. The method further includes transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires.

Jobst discloses a method of transferring a data packet from a providing communication terminal.

9A. Jobst does not teach or disclose transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires cannot render Claim 24 unpatentable

Claim 24 recites, in part, transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires. The Examiner relies on Jobst for rejecting these features.³²

Jobst discloses a method of transferring a data packet from a providing communication terminal to a requesting communication terminal for securing a terminal against unauthorized software loading onto the phone. More particularly, Jobst uses a unique identification code to verify the identity of the requesting communication terminal and thereby check whether the data

³¹ See Office Action dated November 1, 2007, at pages 3 and 22-23.

packet is provided by an authorized provider or not.

After a thorough review of Jobst, Appellants find no support for the rejection. Jobst does not teach or disclose transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires.

The Examiner agreed that Jobst does not explicitly disclose transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires. However, the Examiner states that it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include "transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires" as disclosed by Jobst since a base station transmitting a message to a communication terminal (i.e. mobile station) would have to be received in order to authenticate and verify the communication terminal, prior to the transmission of encryption/decryption information. The Examiner also states that Jobst does suggest a first digital signature and a second digital signature.³³ A rejection based on "a first digital signature and a second digital signature" to reject the claim is not sufficient. The Examiner provides no further support for rejecting these features.

Accordingly, Jobst does not teach or suggest transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires, as recited by Claim 24.

Since Jobst does not teach or suggest the recitation of Claim 24 of the present application, of transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires.

³² See Office Action dated November 1, 2007, at pages 22-23.

³³ See Advisory Action dated February 26, 2008, at page 2 Continuation Sheet.

Based on at least the foregoing it is respectfully submitted that the rejection of Claim 24 under 35 U.S.C. §103(a) must be reversed.

9B. Independent Claim 24 is not rendered obvious by Jobst

The Examiner has failed to show that each and every element of Claim 24, and in as complete detail as is contained therein, are taught in or suggested by the prior art. The Examiner has failed to make out a prima facie case for an obviousness rejection, and thus Claim 24 is allowable.

CONCLUSION


As the Examiner has failed to make out a prima facie case for any of the obviousness rejections, the rejections of Claims 1-7, 9-14 and 16-36 must be reversed.

It is well settled that in order for a rejection under 35 U.S.C. §103(a) to be appropriate, the claimed invention must be shown to be obvious in view of the prior art as a whole. A claim may be found to be obvious if it is first shown that all of the recitations of a claim are taught in the prior art or are suggested by the prior art. In re Royka, 490 F.2d 981, 985, 180 U.S.P.Q. 580, 583 (C.C.P.A. 1974), cited in M.P.E.P. §2143.03.

The Examiner has failed to show that all of the recitations of Claims 1-7, 9-14, 16, 25-36 are taught or suggested by Jobst. Accordingly, the Examiner has failed to make out a prima facie case for an obviousness rejection.

The Examiner has failed to show that all of the recitations of Claims 17-24 are taught or suggested by Jobst. Accordingly, the Examiner has failed to make out a prima facie case for an obviousness rejection. Therefore, the rejections of Claims 1-7, 9-14 and 16-36 must be reversed.

Dated: May 6, 2008

By: 
Paul J. Farrell
Reg. No.: 33,494
Attorney for Appellants

THE FARRELL LAW FIRM, P.C.
333 Earle Ovington Blvd., Suite 701
Uniondale, New York 11553
(516) 228-3565 (tel)
(516) 228-8475 (fax)

CLAIMS APPENDIX

1. (Previously Presented) In a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station, a method for receiving the broadcast service in a mobile station, comprising the steps of:

generating a registration message including a predetermined registration identifier for identification of the encryption information, and transmitting the generated registration message to a base station;

receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station; and

updating the registration identifier based on the updated encryption information.

2. (Original) The broadcast service method of claim 1, wherein the predetermined encryption information includes at least one of a predetermined mask key required for decryption of the broadcast data, generation information for the mask key, and a lifetime of the mask key.

3. (Previously Presented) The broadcast service method of claim 2, wherein the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated.

4. (Previously Presented) The broadcast service method of claim 2, wherein the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated.

5. (Original) The broadcast service method of claim 1, wherein the registration message is a message that is transmitted from the mobile station to the base station for a predetermined time while the mobile station is using a broadcast service.

6. (Original) The broadcast service method of claim 1, wherein the encryption information is generated by a packet data service node and transmitted to the mobile station via the base station.

7. (Original) The broadcast service method of claim 1, wherein the encryption information is generated by the base station and transmitted to the mobile station.

8. (Cancelled)

9. (Previously Presented) In a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, a method for providing by a base station the broadcast service to a mobile station, comprising the steps of:

receiving a registration message transmitted from the mobile station;

determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different from a currently valid registration identifier; and

transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station.

10. (Original) The broadcast service method of claim 9, wherein the predetermined encryption information includes at least one of a predetermined mask key required for decryption of the broadcast data, generation information for the mask key, and a lifetime of the mask key.

11. (Previously Presented) The broadcast service method of claim 10, wherein the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated.

12. (Previously Presented) The broadcast service method of claim 10, wherein the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated.

13. (Original) The broadcast service method of claim 9, further comprising performing an accounting process on the mobile station through a packet data service node when the base station transmits updated encryption information to the mobile station.

14. (Original) The broadcast service method of claim 9, further comprising holding a current state of the mobile station for a predetermined lifetime of the encryption information when the registration identifier of the mobile station is identical to a registration identifier available in the base station.

15. (Cancelled)

16. (Original) The broadcast service method of claim 9, further comprising transmitting a predetermined response message to the mobile station in response to the registration message if it is determined that transmission of the updated encryption information is not necessary.

17. (Previously Presented) In a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station, a method for receiving the broadcast service in a mobile station, comprising the steps of:

generating a registration message including a predetermined mask key request bit for requesting transmission of predetermined mask key for decryption of the broadcast data and transmitting the generated registration message to a base station while the mobile station is using a broadcast service; and

receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit.

18. (Original) The broadcast service method of claim 17, further comprising generating another registration message for requesting a new mask key and transmitting the generated registration message to the base station if the lifetime of the mask key has expired.

19. (Previously Presented) In a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, a method for providing by a base station the broadcast service to a mobile station, comprising the steps of:

receiving a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data, from the mobile station;

analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key; and

transmitting the encryption information to the mobile station when the base station determines to transmit the encryption information.

20. (Previously Presented) In a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data sequentially is encrypted with different encryption information and provided to a mobile station, a method for receiving the broadcast service in the mobile station, comprising the steps of:

generating a registration message for use of the broadcast service and transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires;

receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message; and

continuously decrypting the broadcast data using the next encryption information when the lifetime of the current encryption information expires.

21. (Original) The broadcast service method of claim 20, wherein the predetermined skew time is set to a time longer than a maximum period among registration message transmission periods of all mobile stations receiving a broadcast service in a service area of the base station.

22. (Previously Presented) In a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, a method for providing by a base station the broadcast service to a mobile station, comprising the steps of:

receiving a registration message for use of the broadcast service by the mobile station; and
transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires.

23. (Original) The broadcast service method of claim 22, wherein the skew time is set to a time longer than a maximum period among registration message transmission periods of all mobile stations receiving broadcast service in a service area of the base station.

24. (Previously Presented) In a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, a method for providing by a base station the broadcast service to a mobile station, comprising the steps of:

receiving a predetermined registration message for use of the broadcast service by the mobile station; and

transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires.

25. (Previously Presented) In a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein

broadcast data is sequentially encrypted with different encryption information and provided to a mobile station, a broadcast service method comprising the steps of:

- transmitting, by the mobile station, a first registration message for initial use of the broadcast service to the base station;

- upon receiving the first registration message, transmitting by the base station encryption information for decryption of the broadcast data to the mobile station;

- upon receiving the encryption information, generating by the mobile station a registration identifier which includes identification information of the encryption information;

- generating by the mobile station a second registration message including the registration identifier and transmitting the generated second registration message to the base station if second or later registration for use of the broadcast service by the mobile station is required;

- comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station; and

- transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station.

26. (Original) The broadcast service method of claim 25, further comprising requesting by the base station an accounting process on the mobile station through the packet data service node if the registration identifiers are different.

27. (Original) The broadcast service method of claim 25, further comprising holding by the base station the current encryption information of the mobile station and deferring an accounting process on the mobile station if the registration identifiers are identical.

28. (Original) The broadcast service method of claim 25, wherein the encryption information includes at least one of a predetermined mask key required for decryption of the broadcast data, generation information for the mask key, and a lifetime of the mask key.

29. (Previously Presented) The broadcast service method of claim 28, wherein the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated.

30. (Previously Presented) The broadcast service method of claim 28, wherein the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated.

31. (Previously Presented) A wireless communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station, the system comprising:

at least one mobile station connected to the base station through the radio channel, for performing location registration for use of the broadcast service, decrypting the broadcast data using the encryption information transmitted via the base station while using the broadcast service, generating a registration identifier as identification information of the encryption information, and transmitting the generated registration identifier to the base station; and

at least one base station for transmitting to the mobile station broadcast data transmitted via the packet data service node while the mobile station is using the broadcast service, receiving a predetermined registration message transmitted during location registration of the mobile station, analyzing a registration identifier of the encryption information included in the predetermined registration message, and determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station.

32. (Original) The broadcast service system of claim 31, wherein the registration identifier includes a hash value determined by applying a hash function to a corresponding mask key each time the mask key is updated.

33. (Original) The broadcast service system of claim 31, wherein the registration identifier includes a sequence number sequentially assigned to a corresponding mask key each time the mask key is updated.

34. (Original) The broadcast service system of claim 31, wherein the base station performs an accounting process on the mobile station through the packet data service node when the base station transmitted updated encryption information to the mobile station.

35. (Original) The broadcast service system of claim 32, wherein the base station receives a registration message including a predetermined mask key request bit for requesting transmission of the mask key from the mobile station while the mobile station is using a broadcast service, and transmitting predetermined encryption information including the mask key and lifetime information of the mask key to the mobile station if the mask key request bit has a predetermined bit value.

36. (Original) The broadcast service system of claim 31, wherein the encryption information can be used for decryption of the broadcast data only for a predetermined lifetime, wherein the base station transmits to the mobile station both current encryption information and next encryption information including their lifetimes if it is determined that a registration message of the mobile station was received within a predetermined skew time before a lifetime of current encryption information expires, wherein the mobile station decrypts the broadcast data using the next encryption information when the lifetime of the current encryption information expires.

EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. 1.130, 1.131, 1.132 or entered by the Examiner and relied upon by Appellant.

RELATED PROCEEDINGS APPENDIX

There are no known decisions rendered by a court or the Board in any proceeding identified pursuant to paragraph (c)(1)(ii) of 37 C.F.R. 41.37.